Notice of Allowability	Application No.	Applicant(s)	
	09/807,099	PINKAS ET AL.	
	Examiner	Art Unit	
	HOSUK SONG	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *1/8/07*.

2. ☒ The allowed claim(s) is/are *23-31*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

HOSUK SONG
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Bianco on 3/5/07.

The following claims has been amended as follows:

23. A method for preserving the integrity of a negotiation conducted via a network, ~~such as, the Internet,~~ and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein a trusted entity acting as a center computers and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of participants B.sub.1, B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;

b) secretly generating an input x.sub.i by each participant B.sub.i;

c) publishing by the center A to each participant a commitment to K combinatorial circuits that compute F, where K is a security parameter;

d) transmitting by each participant B.sub.i to the center A a commitment c.sub.i to the value of B.sub.i's input x.sub.i, where c.sub.i is an encryption of x.sub.i;

e) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;

f) providing to each participant B.sub.i part of the K combinatorial circuits that the center A committed to, and requesting center A to open them, whereupon each participant B.sub.i can verify that the part of the circuits opened to participant B.sub.i computes a value F;

g) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment c.sub.i;

h) computing by center A a value of F based on the inputs x.sub.i it received by using a part of the K combinatorial circuits not disclosed to the participants, and publishing the computed value of F to the participants; and

i) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published commitments while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K combinatorial circuits and from their own inputs, and (ii) information about the inputs of the other users.

27. A method for preserving the integrity of a negotiation conducted via a network, ~~such as, the Internet,~~ and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein a trusted entity acting as a center computers and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) announcing by center A that it will compute F;

b) providing an architecture which includes a center A, and a plurality of participants B.sub.1, B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;

c) constructing by center A K garbled circuits including gates having wire inputs and outputs that compute F;

d) choosing by center A a permutation of each wire input of the circuits;

e) publishing by center A to each participant B.sub.i tables of gates, and commitments to the permutations and the garbled values of the input wires;

f) secretly generating an input x.sub.i by each participant B.sub.i;

g) transmitting to center A, for every input wire for every circuit corresponding to an input bit known to participant B.sub.i, a commitment of the permuted value of the input bit:

h) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;

i) selecting by each participant B.sub.i a subset of the K garbled circuits that the center A committed to:

j) revealing by center A its commitments to the subset of the K garbled circuits, whereupon each participant B.sub.i can verify that the circuits revealed to participant B.sub.i computes value F;

k) verifying by participants that test circuits compute F;

l) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment in step g;

m) computing by center A a value of F based on the inputs x.sub.i it received by using circuits not in the subset disclosed to the participants, and publishing the computed value of F to the participants;

n) publishing by center A opened commitments and corresponding garbled inputs; and

o) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published opened commitments and corresponding garbled inputs while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K garbled circuits and from their own inputs, and (ii) information about the inputs of the other users.

31. A method for preserving the integrity of a negotiation conducted via a network, ~~such as, the Internet,~~ and using clients and/or servers, among a plurality of parties each of whom is making a private

input during the transaction and wherein a trusted entity acting as a center computers and outputs a value F of these inputs constituting the output of the transaction comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of participants B.sub.1, B.sub.2,..., B.sub.n, to engage in a transaction during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;

b) secretly generating an input x.sub.i by each participant B.sub.i;

c) publishing by the center A to each participant a commitment to K secure circuits that compute F, where K is a security parameter;

d) transmitting by each participant B.sub.i to the center A a commitment c.sub.i to the value of B.sub.i's input x.sub.i, where c.sub.i is an encryption of x.sub.i;

e) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;

f) providing to each participant B.sub.i part of the K secure circuits that the center A committed to, and requesting center A to open them, whereupon each participant B.sub.i can verify that the part of the circuits opened to participant B.sub.i computes a value F;

g) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment c.sub.i;

h) computing by center A a value of F based on the inputs x.sub.i it received by using a part of the K secure circuits not disclosed to the participants, and publishing the computed value of F to the participants; and

i) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published commitments while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from

the output of the K secure circuits and from their own inputs, and (ii) information about the inputs of the other users.

USPTO Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HOSUK SONG whose telephone number is 5712723857. The examiner can normally be reached on mon-fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KIM VU can be reached on 5712723859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HOSUK SONG
PRIMARY EXAMINER